

Multi-Point AG Codes on the GK Maximal Curves

D. Bartoli, M. Montanucci, and G. Zini

Abstract

In this paper we investigate multi-point Algebraic-Geometric codes associated to the GK maximal curve, starting from a divisor which is invariant under a large automorphism group of the curve. We construct families of codes with large automorphism groups.

1 Introduction

Let \mathcal{X} be an algebraic curve defined over the finite field \mathbb{F}_q of order q . An Algebraic-Geometric code (AG for short) is a linear error correcting code constructed from \mathcal{X} ; see [6, 7]. The parameters of the AG code strictly depend on some characteristics of the underlying curve \mathcal{X} . In general, curves with many \mathbb{F}_q -rational places with respect to their genus give rise to AG codes with good parameters. For this reason maximal curves, that is curves attaining the Hasse-Weil upper bound, have been widely investigated in the literature: for example the Hermitian curve and its quotients, the Suzuki curve, and the Klein quartic; see for instance [8, 14, 15, 17, 19, 21–23]. More recently, AG codes were obtained from the GK curves [5], which are the first example of maximal curves shown not to be covered by the Hermitian curve; see [1, 3].

In this work we investigate multi-point AG codes on the GK curves having a large automorphism group. Note that codes with large automorphism groups can have good performance in encoding [9] and decoding [11].

Most of the AG codes described in the literature are one-point or two-point. A natural way to get AG codes with large automorphism groups is to construct them from a divisor of \mathcal{X} which is invariant under an automorphism group of \mathcal{X} ; see for instance [2, 12, 13].

The main result of the paper is the construction of some families of $[n, k, d]_q$ -codes as AG codes on the GK curve \mathcal{X} of genus $g = \frac{q^5 - 2q^3 + q^2}{2}$. The results are summarized in the Table 1; they depend on non-negative integers m , s , and $r := \gcd\left(s, \frac{q^2 - q + 1}{\gcd(3, q + 1)}\right)$.

Table 1: Parameters of the constructed codes

Code	n	d	m	k	Automorphism group
C (Sect. 3)	$q^8 - q^6 + q^5 - q^3$	d^*	$[q^2 - 1, q^5 - q^3 - 1]$	$m(q^3 + 1) + 1 - g$	
			$[2, q^2 - 1]$	$\leq m(q^3 + 1) + 1 - g$	$(\text{Aut}(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*$
\bar{C} (Sect. 4.1)	$q^8 - q^6 + q^5$ $-(s + 1)q^3$, with $s > 0$	$\geq d^*$	$\left[\frac{q^5 - 2q^3 + q^2 - 1}{(s + 1)q^3 + 1}, \frac{q^8 - q^6 + q^5 - (s + 1)q^3 - 1}{(s + 1)q^3 + 1} \right]$	$m(s + 1)q^3 + m$ $+ 1 - g$	
			$\left[2, \frac{q^8 - q^6 + q^5 - (s + 1)q^3}{(s + 1)q^3(q^3 + 1)} \right]$	$\leq m(s + 1)q^3 + m$ $+ 1 - g$	$((\text{SU}(3, q) \times C_r) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*$
\tilde{C} (Sect. 4.2)	$q^8 - q^6 + q^5$ $-(s + 1)q^3 + 1$	d^*	$\left[\frac{q^5 - 2q^3 + q^2 - 1}{(s + 1)q^3}, \frac{q^5 - q^3 + q^2}{s + 1} - 1 \right]$	$m(s + 1)q^3$ $+ 1 - g$	$((Q_{q^3} \rtimes H_{q^2 - 1}) \times C_{q^2 - q + 1}) \rtimes \text{Aut}(\mathbb{F}_{q^6}) \rtimes \mathbb{F}_{q^6}^*,$ if $s = 0$
			$\left[2, \frac{q^5 - q^3 + q^2 - (s + 1)}{(s + 1)(q^3 + 1)} \right]$	$\leq m(s + 1)q^3$ $+ 1 - g$	$((Q_{q^3} \rtimes H_{q^2 - 1}) \times C_r) \rtimes \text{Aut}(\mathbb{F}_{q^6}) \rtimes \mathbb{F}_{q^6}^*,$ if $s > 0$ and $p \nmid m$

In Section 2 we introduce basic notions and preliminary results concerning AG codes and GK curves. Sections 3 and 4 contain the main achievements of this paper.

2 Background and preliminary results

2.1 Algebraic Geometric codes

In this section we introduce some basic notions on AG codes. For a more detailed introduction on this topic we refer to [18].

Let \mathcal{X} be a projective curve over \mathbb{F}_q , and consider the field of rational functions $\mathbb{F}_q(\mathcal{X})$ on \mathcal{X} . Let $\mathcal{X}(\mathbb{F}_q)$ be the set of all the \mathbb{F}_q -rational places of \mathcal{X} . Given an \mathbb{F}_q -rational divisor $D = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} n_P P$ on \mathcal{X} , the Riemann-Roch space $\mathcal{L}(D)$ is a finite dimensional \mathbb{F}_q -vector space given by

$$\mathcal{L}(D) := \{f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \geq 0\} \cup \{0\},$$

where (f) indicates the principal divisor of f .

Let $D = P_1 + \cdots + P_n$, with $P_i \neq P_j$ for $i \neq j$, be an \mathbb{F}_q -rational divisor where each P_i has weight one in D . Let G be another \mathbb{F}_q -rational divisor of $\mathbb{F}_q(\mathcal{X})$ such that $\text{supp}(D) \cap \text{supp}(G) = \emptyset$. The *functional code* $C_{\mathcal{L}}(D, G)$ is defined as follows. Consider the evaluation map

$$\begin{aligned} e_D : \mathcal{L}(G) &\rightarrow \mathbb{F}_q^n \\ f &\mapsto e_D(f) = (f(P_1), f(P_2), \dots, f(P_n)) \end{aligned}$$

The map e_D is \mathbb{F}_q -linear and injective if $n > \deg(G)$. We define $C_{\mathcal{L}}(D, G) = e_D(\mathcal{L}(G))$, an $[n, k, d]_q$ code with $k = \ell(G) - \ell(G - D)$ and $d \geq d^* = n - \deg(G)$. The integer d^* is called *designed minimum distance*. If $\deg(G) > 2g - 2$, where g is the genus of the curve \mathcal{X} , then $k = \deg(G) + 1 - g$. The *differential code* $C_{\Omega}(D, G)$ is defined as

$$C_{\Omega}(D, G) = \{(\text{res}_{P_1}(\omega), \text{res}_{P_2}(\omega), \dots, \text{res}_{P_n}(\omega) \mid \omega \in \Omega(G - D)\},$$

where $\Omega(G - D) = \{\omega \in \Omega(\mathcal{X}) \mid (\omega) \geq G - D\} \cup \{0\}$. The differential code $C_{\Omega}(D, G)$ has dimension $n - \deg(G) + g - 1$ and minimum distance at least $\deg(G) - 2g + 2$.

Now we define the automorphism group of $C_{\mathcal{L}}(D, G)$; see [4, 12]. Let $\mathcal{M}_{n,q} \leq \text{GL}(n, q)$ be the subgroup of matrices having exactly one non-zero element in each row and column. For $\gamma \in \text{Aut}(\mathbb{F}_q)$ and $M = (m_{i,j})_{i,j} \in \text{GL}(n, q)$, let M^{γ} be the matrix $(\gamma(m_{i,j}))_{i,j}$. Let $\mathcal{W}_{n,q}$ be the semidirect product $\mathcal{M}_{n,q} \rtimes \text{Aut}(\mathbb{F}_q)$ with multiplication $M_1 \gamma_1 \cdot M_2 \gamma_2 := M_1 M_2^{\gamma_1} \cdot \gamma_1 \gamma_2$. The *automorphism group* $\text{Aut}(C_{\mathcal{L}}(D, G))$ of $C_{\mathcal{L}}(D, G)$ is the subgroup of $\mathcal{W}_{n,q}$ preserving $C_{\mathcal{L}}(D, G)$, that is,

$$M\gamma(x_1, \dots, x_n) := ((x_1, \dots, x_n) \cdot M)^{\gamma} \in C_{\mathcal{L}}(D, G) \text{ for any } (x_1, \dots, x_n) \in C_{\mathcal{L}}(D, G).$$

Let $\text{Aut}_{\mathbb{F}_q}(\mathcal{X})$ be the \mathbb{F}_q -automorphism group of \mathcal{X} ,

$$\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X}) := \{\sigma \in \text{Aut}_{\mathbb{F}_q}(\mathcal{X}) \mid \sigma(D) = D, \sigma(G) \approx_D G\},$$

where $G' \approx_D G$ if and only if there exists $u \in \mathbb{F}_q(\mathcal{X})$ such that $G' - G = (u)$ and $u(P_i) = 1$ for $i = 1, \dots, n$, and

$$\text{Aut}_{\mathbb{F}_q, D, G}^+(\mathcal{X}) := \{\sigma \in \text{Aut}_{\mathbb{F}_q}(\mathcal{X}) \mid \sigma(D) = D, \sigma(|G|) = |G|\},$$

where $|G| = \{G + (f) \mid f \in \overline{\mathbb{F}_q}(\mathcal{X})\}$ is the linear series associated with G . Note that $\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X}) \subseteq \text{Aut}_{\mathbb{F}_q, D, G}^+(\mathcal{X})$.

Remark 2.1. Suppose that $\text{supp}(D) \cup \text{supp}(G) = \mathcal{X}(\mathbb{F}_q)$ and each place in $\text{supp}(G)$ has the same weight in G . Then

$$\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X}) = \text{Aut}_{\mathbb{F}_q, D, G}^+(\mathcal{X}) = \{\sigma \in \text{Aut}_{\mathbb{F}_q}(\mathcal{X}) \mid \sigma(\text{supp}(G)) = \text{supp}(G)\}.$$

In [4] the following result was proved.

Theorem 2.2. ([4, Theorem 3.4]) Suppose that the following conditions hold:

- G is effective;
- $\ell(G - P) = \ell(G) - 1$ and $\ell(G - P - Q) = \ell(G) - 2$ for any $P, Q \in \mathcal{X}$;
- \mathcal{X} has a plane model $\Pi(\mathcal{X})$ with coordinate functions $x, y \in \mathcal{L}(G)$;
- \mathcal{X} is defined over \mathbb{F}_p ;
- the support of D is preserved by the Frobenius morphism $(x, y) \mapsto (x^p, y^p)$;
- $n > \deg(G) \cdot \deg(\Pi(\mathcal{X}))$.

Then

$$\text{Aut}(C_{\mathcal{L}}(D, G)) \cong (\text{Aut}_{\mathbb{F}_q, D, G}^+(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_q)) \rtimes \mathbb{F}_q^*.$$

In the construction of AG codes, the condition $\text{supp}(D) \cap \text{supp}(G) = \emptyset$ can be removed as follows; see [20, Sec. 3.1.1]. Let P_1, \dots, P_n be distinct \mathbb{F}_q -rational places of \mathcal{X} and $D = P_1 + \dots + P_n$, $G = \sum n_P P$ be \mathbb{F}_q -rational divisors of \mathcal{X} . For any P_i let $b_i = n_{P_i}$ and t_i be a local parameter at P_i . The map

$$\begin{aligned} e'_D : \mathcal{L}(G) &\rightarrow \mathbb{F}_q^n \\ f &\mapsto e'_D(f) = ((t^{b_1} f)(P_1), (t^{b_2} f)(P_2), \dots, (t^{b_n} f)(P_n)) \end{aligned}$$

is linear. We define the *extended AG code* $C_{ext}(D, G) := e'(\mathcal{L}(G))$. Note that e'_D is not well-defined since it depends on the choice of the local parameters; yet, different choices yield extended AG codes which are equivalent. The code C_{ext} is a lengthening of $C_{\mathcal{L}}(\hat{D}, G)$, where $\hat{D} = \sum_{P_i: n_{P_i}=0} P_i$. The extended code C_{ext} is an $[n, k, d]_q$ -code for which the following properties still hold:

- $d \geq d^* := n - \deg(G)$.
- $k = \ell(G) - \ell(G - D)$.
- If $n > \deg(G)$, then $k = \ell(G)$; if $n > \deg(G) > 2g - 2$, then $k = \deg(G) + 1 - g$.

2.2 The Giulietti-Korchmáros curve

Let q be a prime power. The GK curve \mathcal{X} over \mathbb{F}_{q^6} is a non-singular curve of $PG(3, \mathbb{F}_q)$ defined by the affine equations

$$\begin{cases} Y^{q+1} = X^q + X \\ Z^{q^2-q+1} = Y^{q^2} - Y \end{cases} \quad (1)$$

This curve has genus $g = \frac{(n^3+1)(n^2-2)}{2} + 1$, $q^8 - q^6 + q^5 + 1$ \mathbb{F}_{q^6} -rational points, and a unique point at infinity P_∞ , which is \mathbb{F}_{q^2} -rational. The curve \mathcal{X} has been introduced in [5], where it was proved that \mathcal{X} is maximal over \mathbb{F}_{q^6} , that is, the number $|\mathcal{X}(\mathbb{F}_{q^6})|$ of \mathbb{F}_{q^6} -rational points of \mathcal{X} equals $q^6 + 1 + 2gq^3$. Also, for $q > 2$, \mathcal{X} is not \mathbb{F}_{q^6} -covered by the Hermitian curve maximal over \mathbb{F}_{q^6} ; \mathcal{X} was the first maximal curve shown to have this property.

The automorphism group $\text{Aut}(\mathcal{X})$ of \mathcal{X} is defined over \mathbb{F}_{q^6} and has size $q^3(q^3 + 1)(q^2 - 1)(q^2 - q + 1)$. In particular, it has a normal subgroup isomorphic to $\text{SU}(3, q)$. If $(3, q+1) = 1$, then $\text{Aut}(\mathcal{X}) \cong \text{SU}(3, q) \times C_{q^2-q+1}$, where C_{q^2-q+1} is a cyclic group of order $q^2 - q + 1$. If $(3, q+1) = 3$, then $\text{SU}(3, q) \times C_{(q^2-q+1)/3}$ is isomorphic to a normal subgroup of $\text{Aut}(\mathcal{X})$ of index 3; see [5, Theorem 6]. The set $\mathcal{X}(\mathbb{F}_{q^6})$ of the \mathbb{F}_{q^6} -rational points of \mathcal{X} splits into two orbits under the action of $\text{Aut}(\mathcal{X})$: one orbit $\mathcal{O}_1 = \mathcal{X}(\mathbb{F}_{q^2})$ of size $q^3 + 1$, which coincides with the intersection between \mathcal{X} and the plane $Z = 0$; the other orbit $\mathcal{O}_2 = \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ of size $q^3(q^3 + 1)(q^2 - 1)$; see [5, Theorem 7].

By the Orbit-Stabilizer Theorem, the stabilizer $\text{Aut}(\mathcal{X})_{P_\infty}$ of P_∞ in $\text{Aut}(\mathcal{X})$ has order $q^3(q^2 - 1)(q^2 - q + 1)$. By direct checking, $\text{Aut}(\mathcal{X})_{P_\infty} < \text{SU}(3, q) \times C_{(q^2-q+1)/\delta}$ where $\delta = (3, q+1)$, and $\text{Aut}(\mathcal{X})_{P_\infty}$ contains a subgroup $(Q_{q^3} \rtimes H_{q^2-1}) \times C_{(q^2-q+1)/\delta}$ of index δ . Here, Q_{q^3} is a Sylow p -subgroup of $\text{Aut}(\mathcal{X})$ and H_{q^2-1} is a cyclic group of order $q^2 - 1$; see Lemma 8 and the subsequent discussion in [5].

Let $x, y, z \in \mathbb{F}_{q^6}(\mathcal{X})$ be the coordinate functions of the function field of \mathcal{X} , which satisfy $y^{q+1} = x^q + x$ and $z^{q^2-q+1} = y^{q^2} - y$. Also, denote by P_0 and $P_{(a,b,c)}$ the affine points $(0, 0, 0)$ and (a, b, c) respectively. Then it is not difficult to prove that

- $(x) = (q^3 + 1)P_0 - (q^3 + 1)P_\infty$;
- $(y) = (q^2 - q + 1)(\sum_{a: a^q + a = 0} P_{(a,0,0)}) - (q^3 - q^2 + q)P_\infty$;
- $(z) = (\sum_{P \in \mathcal{X}(\mathbb{F}_{q^2}), P \neq P_\infty} P) - q^3 P_\infty$.

3 AG codes on the GK curves

Let $m \in \mathbb{N}$ and consider the sets

$$\mathcal{G} := \mathcal{X}(\mathbb{F}_{q^2}), \quad \mathcal{D} := \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{G}.$$

Note that \mathcal{G} is the intersection of \mathcal{X} with the plane $Z = 0$. Define the \mathbb{F}_{q^6} -divisors

$$G := \sum_{P \in \mathcal{G}} mP \quad \text{and} \quad D := \sum_{P \in \mathcal{D}} P,$$

which have degree $m(q^3 + 1)$ and $q^8 - q^6 + q^5 - q^3$, respectively. Denote by $C := C_{\mathcal{X}}(D, G)$ the associated functional AG code over \mathbb{F}_{q^6} having length $n = q^8 - q^6 + q^5 - q^3$, dimension k , and minimum distance d . The designed minimum distance of C is

$$d^* = n - \deg G = q^8 - q^6 + q^5 - q^3 - m(q^3 + 1).$$

Lemma 3.1. *There exist exactly $q^5 - q^3$ planes $\pi_a : X = a$, $a \in \mathbb{F}_{q^6}$, containing $q^3 + 1$ distinct \mathbb{F}_{q^6} -rational points of \mathcal{X} . Their affine points give rise to a partition of $\mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$.*

Proof. Let $a \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ such that \mathcal{X} contains an \mathbb{F}_{q^6} -rational point (a, b, c) . Then $b, c \neq 0$, and $\pi_a \cap \mathcal{X}$ has exactly $q^3 + 1$ affine distinct points, namely $\pi_a \cap \mathcal{X} = \{(a, \xi b, \eta c) \mid \xi^{q+1} = \eta^{q^2-q+1} = 1\}$. Now let $a \in \mathbb{F}_{q^2}$. Then $(a, b, c) \in \mathcal{X}$ if and only if $b, c \in \mathbb{F}_{q^2}$ satisfy $b^{q+1} = a^q + a$ and $c = 0$. In particular, $\pi_a \cap \mathcal{X}$ has either 1 or $q + 1$ affine points, according to $a^q + a = 0$ or $a^q + a \neq 0$, respectively. Therefore the number of planes π_a intersecting \mathcal{X} in exactly $q^3 + 1$ \mathbb{F}_{q^6} -rational points is $|\text{supp}(D)|/|\pi_a \cap \mathcal{X}| = \frac{q^8 - q^6 + q^5 - q^3}{q^3 + 1} = q^5 - q^3$. \square

Now we show that the designed minimum distance is attained by C .

Proposition 3.2. *Whenever $d^* > 0$, C attains the designed minimum distance d^* .*

Proof. Take m distinct elements $a_1, \dots, a_m \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ such that $|\pi_a \cap \mathcal{X}| = q^3 + 1$, and let

$$f := \prod_{i=1}^m \left(\frac{x - a_i}{z} \right). \quad (2)$$

Then the pole divisor of f is $(f)_\infty = G$, thus $f \in \mathcal{L}(G)$. The weight of $e_D(f)$ is

$$w(e_D(f)) = n - m(q^3 + 1) = d^*.$$

□

When m is in a suitable range, the dimension of C can be explicitly computed.

Proposition 3.3. *If $q^2 - 1 \leq m \leq q^5 - q^3 - 1$, then*

$$k = m(q^3 + 1) - \frac{1}{2}(q^5 - 2q^3 + q^2 - 2).$$

Proof. Since $n > \deg G > 2g - 2$, then by Riemann-Roch Theorem $k = \deg G + 1 - g$. □

Let H be the \mathbb{F}_{q^2} -divisor given by $H := \sum_{P \in G} P$, so that $G = mH$.

Proposition 3.4. *If $m < q^5 - q^3 + q^2 - 2$, then the codes $C_\Omega(D, G)$ and $C_{\mathcal{L}}(D, (q^5 - q^3 + q^2 - m - 2)H)$ are monomially equivalent.*

Proof. From [16, Chapter 12.17], $C_\Omega(D, G) = C_{\mathcal{L}}(D, K + D - G)$ for any canonical divisor K . The function z has valuation 1 at each affine \mathbb{F}_{q^6} -rational point of \mathcal{X} , hence z is a separating element for $\overline{\mathbb{F}_{q^6}}(\mathcal{X})/\overline{\mathbb{F}_{q^6}}$ by [18, Prop. 3.10.2]. Then dz is non-zero by [18, Prop. 4.1.8(c)]. It is easily checked that (dz) is a one-point divisor at P_∞ . Therefore, we may choose $K = (dz) = (q^3 + 1)(q^2 - 2)P_\infty$.

It suffices to prove that $K + D - G \equiv (q^5 - q^3 + q^2 - m - 2)H$, that is,

$$K + D \equiv (q^5 - q^3 + q^2 - 2)H.$$

Let π_{a_i} , $i = 1, \dots, q^5 - q^3$, be the $q^5 - q^3$ planes described in Lemma 3.1. Consider the function

$$f := \left(\prod_{i=1}^{q^5 - q^3} (x - a_i) \right) \left(\prod_{P \in \text{supp}(G), P \neq P_\infty} \tau_P(x, y) \right),$$

where $\tau_P(x, y) \in \mathbb{F}_{q^2}[x, y]$ has principal divisor $(\tau_P) = (q^3 + 1)P - (q^3 + 1)P_\infty$, that is, $\tau_P(X, Y)$ is the tangent plane to \mathcal{X} at P . Then

$$K + D - (q^5 - q^3 + q^2 - 2)H = \text{div} \left(\frac{f}{z^{q^5 + q^2 - 1}} \right).$$

Hence the claim follows. □

We determine the automorphism group of C . To this aim, we prove a preliminary Lemma.

Lemma 3.5. *Let $m \geq 2$. For any $P, Q \in \mathcal{X}$, $\ell(G-P) = \ell(G)-1$ and $\ell(G-P-Q) = \ell(G)-2$.*

Proof. When P and Q are affine points, we denote their coordinates by (a, b, c) and $(\bar{a}, \bar{b}, \bar{c})$, respectively. The condition $\ell(G-P-Q) = \ell(G)-2$ implies $\ell(G-P) = \ell(G)-1$ (see [18, Lemma 1.4.8]), hence we restrict to the condition on two points. To prove the claim, we provide two \mathbb{F}_{q^6} -linearly independent functions $f_1, f_2 \in \mathcal{L}(G)$ such that $f_1, f_2 \notin \mathcal{L}(G-P-Q)$ and $f_1 + \lambda f_2 \notin \mathcal{L}(G-P-Q)$ for any $\lambda \in \mathbb{F}_{q^6}$.

- Case $P, Q \notin \text{supp}(G)$, $P \neq Q$. If $c \neq \bar{c}$, choose $f_1 = \frac{z-\alpha}{z}$, $f_2 = \frac{z-\beta}{z}$ with $\alpha \neq \beta$, $\alpha, \beta \notin \{c, \bar{c}, 0\}$. If $c = \bar{c}$, then $a \neq \bar{a}$; choose $f_1 = \frac{x-\alpha}{z^2}$, $f_2 = \frac{x-\beta}{z^2}$ with $\alpha \neq \beta$, $\alpha, \beta \notin \{a, \bar{a}, 0\}$.
- Case $P, Q \notin \text{supp}(G)$, $P = Q$. Choose $f_1 = \frac{z-c}{z}$, $f_2 = \frac{z-\alpha}{z}$ with $\alpha \notin \{c, 0\}$.
- Case $P \in \text{supp}(G)$, $Q \notin \text{supp}(G)$, $P \neq P_\infty$. Choose $f_1 = \left(\frac{z-\bar{c}}{z-c}\right)^m$, $f_2 = \left(\frac{z-\alpha}{z-c}\right)^m$ with $\alpha \notin \{\bar{c}, c\}$.
- Case $P = P_\infty$, $Q \notin \text{supp}(G)$. Choose $f_1 = \left(\frac{x}{z}\right)^m$, $f_2 = \left(\frac{x-\bar{a}}{z}\right)^m$.
- Case $P, Q \in \text{supp}(G) \setminus \{P_\infty\}$, $P \neq Q$. Since $a \neq \bar{a}$, we can choose $f_1 = \left(\frac{x-a}{z-c}\right)^m$, $f_2 = \left(\frac{x-\alpha}{z-c}\right)^m$ with $\alpha \neq a$.
- Case $P = P_\infty$, $Q \in \text{supp}(G) \setminus \{P_\infty, O\}$. Choose $f_1 = \left(\frac{x}{z-c}\right)^m$, $f_2 = \left(\frac{x-\bar{a}}{z-c}\right)^m$.
- Case $P = P_\infty$, $Q = O$. Choose $f_1 = \left(\frac{x}{z}\right)^m$, $f_2 = \left(\frac{x-\alpha}{z}\right)^m$ with $\alpha \neq 0$.
- Case $P = Q \in \text{supp}(G) \setminus \{P_\infty\}$. Choose $f_1 = \frac{z-\alpha}{z^m}$, $f_2 = \frac{z-\beta}{z^m}$ with $\alpha \neq \beta$ and $\alpha, \beta \neq 0$.
- Case $P = Q = P_\infty$. Choose $f_1 = \left(\frac{x}{z}\right)^m$, $f_2 = \left(\frac{x}{z}\right)^{m-1}$.

By direct checking, in each case we have $f_1, f_2 \in \mathcal{L}(G)$, $f_1, f_2 \notin \mathcal{L}(G-P-Q)$, and $f_1 + \lambda f_2 \notin \mathcal{L}(G-P-Q)$ for any $\lambda \in \mathbb{F}_{q^6}$. The claim follows. \square

Proposition 3.6. *If $2 \leq m \leq q^2 - 1$, then the automorphism group of C is*

$$\text{Aut}(C) \cong (\text{Aut}(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

In particular, $\text{Aut}(C)$ has order $6q^3(q+1)^3(q-1)^2(q^2-q+1)^3(q^2+q+1)\log_p(q)$.

Proof. The following properties hold.

- The divisor G is effective.
- By Lemma 3.5, $\ell(G - P) = \ell(G) - 1$ and $\ell(G - P - Q) = \ell(G) - 2$ for any $P, Q \in \mathcal{X}$.
- Let $\Pi(\mathcal{X})$ be the plane model of \mathcal{X} given in [5, Theorem 4], which has degree $q^3 + 1$. The function field $\overline{\mathbb{F}}_{q^6}(\Pi(\mathcal{X}))$ is generated by the coordinate functions x and z , hence also by $x' := x/z^2$ and $z' := 1/z$. The pole divisors of x' and z' are

$$(z')_\infty = \sum_{P \in \mathcal{G}, P \neq P_\infty} P, \quad (x')_\infty = \sum_{P \in \mathcal{G}, P \neq P_\infty, P \neq O} 2P,$$

where $O = (0, 0, 0)$. Thus $x', z' \in \mathcal{L}(G)$.

- The curve \mathcal{X} is defined over \mathbb{F}_p .
- The Frobenius morphism $\Phi_p : (x, z) \mapsto (x^p, z^p)$ on $\Pi(\mathcal{X})$ preserves $\mathcal{X}(\mathbb{F}_{q^6})$ and $\mathcal{X}(\mathbb{F}_{q^2})$, hence also the support $\mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ of D .
- The condition $n > \deg G \cdot \deg(\Pi(\mathcal{X}))$ holds if and only if $m \leq n^2 - 1$.

Then by Theorem 2.2 we have

$$\text{Aut}(C) \cong (\text{Aut}_{\mathbb{F}_{q^6}, D, G}^+(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

By Remark 2.1, $\text{Aut}_{\mathbb{F}_{q^6}, D, G}^+(\mathcal{X}) \cong \text{Aut}_{\mathbb{F}_{q^6}, D, G}(\mathcal{X})$, and both coincide with $\text{Aut}_{\mathbb{F}_{q^6}}(\mathcal{X})$. Since $\text{Aut}(\mathcal{X})$ is defined over \mathbb{F}_{q^6} , the claim follows. \square

We construct a lengthening of C by extending D to the support of G .

Define the \mathbb{F}_{q^6} -divisors $G' := G$ and $D' := \sum_{P \in \mathcal{X}(\mathbb{F}_{q^6})} P$ having degree $m(q^3 + 1)$ and $q^8 - q^6 + q^5 + 1$, respectively. Denote by $C' := C_{\text{ext}}(D', G')$ the associated extended AG code over \mathbb{F}_{q^6} having length $n' = q^8 - q^6 + q^5 + 1$, dimension k' , and designed minimum distance $d'^* = n' - \deg(G') = q^8 - q^6 + q^5 - mq^3 - m + 1$.

Lemma 3.7. *Whenever $d'^* > 0$, C' attains the designed minimum distance d'^* .*

Proof. Let $f \in \mathcal{L}(G')$ be defined as in (2). The codewords $e'_{D'} \in C'$ and $e_D \in C$ have the same number $m(q^3 + 1)$ of zero coordinates, hence the weight of $e'_{D'}$ is $n' - \deg(G') = d'^*$. \square

In particular, $n' - d' = n - d$. The proof of the following result is analogous to the one of Proposition 3.3.

Proposition 3.8. *If $q^2 - 1 \leq m \leq q^5 - q^3$, then $k' = m(q^3 + 1) - \frac{1}{2}(q^5 - 2q^3 + q^2 - 2)$.*

Therefore, if $q^2 - 1 \leq m \leq q^5 - q^3 - 1$, then C and C' have the same Singleton defect.

4 Some other constructions

For $c \in \mathbb{F}_{q^6}$, let ζ_c be the plane with affine equation $Z = c$, and

$$\Gamma := \left\{ c \in \mathbb{F}_{q^6} \mid c^{(q^3+1)(q^2-1)} + c^{(q^3+1)(q^2-q)} + 1 = 0 \right\}, \quad \Gamma_0 := \Gamma \cup \{0\}.$$

Lemma 4.1. *The plane ζ_c contains q^3+1 \mathbb{F}_{q^6} -rational points of \mathcal{X} if and only if $c \in \Gamma_0$. The number of such planes is $q^5 - q^3 + q^2$, and their affine points form a partition of $\mathcal{X}(\mathbb{F}_{q^6}) \setminus \{P_\infty\}$.*

Proof. For any c , $P_\infty \in \zeta_c$. We prove that the equations

$$y^{q^2} - y - c^{q^2-q+1} = 0, \quad x^q + x - y^{q+1} = 0$$

have q^3 solutions $(x, y) \in \mathbb{F}_{q^6}^2$ if and only if $c \in \Gamma_0$. By [10, Theorem 1.22], the equation

$$y^{q^2} - y - c^{q^2-q+1} = 0 \tag{3}$$

has q^2 distinct solutions $y \in \mathbb{F}_{q^6}$ if and only if

$$(c^{q^2-q+1})^{q^4} + (c^{q^2-q+1})^{q^2} + c^{q^2-q+1} = 0, \tag{4}$$

and the equation $x^q + x - y^{q+1} = 0$ has q distinct solution $x \in \mathbb{F}_{q^6}$ if and only if

$$-y^{q+1} + (y^{q+1})^q - (y^{q+1})^{q^2} + (y^{q+1})^{q^3} - (y^{q+1})^{q^4} + (y^{q+1})^{q^5} = 0. \tag{5}$$

Using (3), Equation (5) reads

$$c^{(q^3+1)q^2} + c^{(q^3+1)(q^2-q+1)} + c^{q^3+1} = 0. \tag{6}$$

By direct computation, every solution c of Equation (6) is also a solution of Equation (4); also, $c \in \mathbb{F}_{q^6}$. Since the polynomial $c^{(q^3+1)(q^2-1)} + c^{(q^3+1)(q^2-q)} + 1$ is separable, the solutions are all distinct. By the Hasse-Weil bound, $|\mathcal{X}(\mathbb{F}_{q^6}) \setminus \{P_\infty\}| = q^3|\Gamma_0|$, and the claim follows. \square

4.1 First construction

Let $\bar{m}, \bar{s} > 0$ and take $\bar{s} + 1$ distinct elements $c_0 = 0, c_1, \dots, c_{\bar{s}} \in \Gamma_0$. Define the sets

$$\bar{\mathcal{G}} := \bigcup_{i=0}^{\bar{s}} (\mathcal{X} \cap \zeta_{c_i}), \quad \bar{\mathcal{D}} := \mathcal{X}(\mathbb{F}_{q^6}) \setminus \bar{\mathcal{G}}$$

and the \mathbb{F}_{q^6} -divisors

$$\bar{G} := \bar{m}(P_\infty + \sum_{P \in \bar{\mathcal{G}}, P \neq P_\infty} P), \quad \bar{D} := \sum_{P \in \bar{\mathcal{D}}} P,$$

which have degree $\bar{m} + \bar{m}(\bar{s} + 1)q^3$ and $q^8 - q^6 + q^5 - (\bar{s} + 1)q^3$, respectively. Denote by $\bar{C} := C_{\mathcal{L}}(\bar{D}, \bar{G})$ the associated functional AG code over \mathbb{F}_{q^6} having length $\bar{n} = \deg \bar{D}$, dimension \bar{k} , and minimum distance \bar{d} . The designed minimum distance of \bar{C} is

$$\bar{d}^* = \bar{n} - \deg \bar{G} = q^8 - q^6 + q^5 - (\bar{m} + 1)(\bar{s} + 1)q^3 - \bar{m}$$

Proposition 4.2. *If $\frac{q^5 - 2q^3 + q^2 - 1}{(\bar{s} + 1)q^3 + 1} \leq \bar{m} \leq \frac{q^8 - q^6 + q^5 - (\bar{s} + 1)q^3 - 1}{(\bar{s} + 1)q^3 + 1}$, then*

$$\bar{k} = \bar{m} \left(1 + (\bar{s} + 1)q^3 \right) - \frac{1}{2} (q^5 - 2q^3 + q^2 - 2).$$

Proof. The proof is analogous to the proof of Proposition 3.3. \square

Lemma 4.3. *Let $\bar{m} \geq 2$. For any $P, Q \in \mathcal{X}$, $\ell(\bar{G} - P) = \ell(\bar{G}) - 1$ and $\ell(\bar{G} - P - Q) = \ell(\bar{G}) - 2$.*

Proof. We argue as in the proof of Lemma 3.5. When $P, Q \neq P_\infty$, let $P = (a, b, c)$, $Q = (\bar{a}, \bar{b}, \bar{c})$. It is enough to prove the condition on two points, by providing two \mathbb{F}_{q^6} -linearly independent functions $f_1, f_2 \in \mathcal{L}(\bar{G})$ such that $f_1, f_2 \notin \mathcal{L}(\bar{G} - P - Q)$ and $f_1 + \lambda f_2 \notin \mathcal{L}(\bar{G} - P - Q)$ for any $\lambda \in \mathbb{F}_{q^6}$.

- Case $P \notin \text{supp}(\bar{G})$ or $Q \notin \text{supp}(\bar{G})$. Argue as in the proof of Lemma 3.5.
- Case $P, Q \in \text{supp}(\bar{G}) \setminus \{P_\infty\}$, $P \neq Q$. If $c \neq \bar{c}$, assume without loss of generality that $c \neq 0$ and choose $f_1 = \left(\frac{z-c}{z}\right)^m$, $f_2 = \left(\frac{z-\alpha}{z}\right)^m$ with $\alpha \notin \{c, 0\}$; if $c = \bar{c}$, then $a \neq \bar{a}$ and choose $f_1 = \frac{x-a}{(z-c_i)^m}$, $f_2 = \frac{x-\bar{a}}{(z-c_i)^m}$ with $i \in \{0, 1, \dots, \bar{s}\}$, $c_i \neq c$.
- Case $P = P_\infty$. Argue as in the proof of Lemma 3.5.
- Case $P = Q \in \text{supp}(\bar{G}) \setminus \{P_\infty\}$. Choose $f_1 = \frac{z-\alpha}{z^m}$, $f_2 = \frac{z-\beta}{z^m}$ with $\alpha \neq \beta$ and $\alpha, \beta \notin \{c_0, c_1, \dots, c_s\}$.

\square

Proposition 4.4. *Let $2 \leq \bar{m} \leq \frac{q^8 - q^6 + q^5 - (\bar{s} + 1)q^3}{(\bar{s} + 1)q^3(q^3 + 1)}$ and $r := \gcd\left(s, \frac{q^2 - q + 1}{\delta}\right)$, where $\delta := \gcd(3, q + 1)$. Suppose that $\{c_1, \dots, c_s\}$ is closed under the Frobenius map $c_i \mapsto c_i^p$ and under the scalar map $\Lambda : c_i \mapsto \lambda c_i$, where $\lambda^r = 1$. Then the automorphism group of \bar{C} is*

$$\text{Aut}(\bar{C}) \cong ((\text{SU}(3, q) \times C_r) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*$$

of order $r q^3 (q + 1)^3 (q - 1)^2 (q^2 - q + 1)^2 (q^2 + q + 1) \log_p(q^6)$.

Proof. We argue as in the proof of Proposition 3.6.

- The divisor \bar{G} is effective.
- By Lemma 4.3, $\ell(\bar{G} - P) = \ell(\bar{G}) - 1$ and $\ell(\bar{G} - P - Q) = \ell(\bar{G}) - 2$ for any $P, Q \in \mathcal{X}$.
- Let $\Pi(\mathcal{X})$ be the plane model of \mathcal{X} given in [5, Theorem 4], which has degree $q^3 + 1$. The function field $\mathbb{F}_{q^6}(\Pi(\mathcal{X}))$ is generated by the functions $x' := x/z^2$ and $z' := 1/z$. We have $x', z' \in \mathcal{L}(\bar{G})$.
- The curve \mathcal{X} is defined over \mathbb{F}_p .
- The Frobenius morphism $\Phi_p : (x, z) \mapsto (x^p, z^p)$ on $\Pi(\mathcal{X})$ preserves the support of \bar{G} by hypothesis, hence also the support of D .
- The condition $\bar{n} > \deg \bar{G} \cdot \deg(\Pi(\mathcal{X}))$ holds if and only if $m \leq \frac{q^8 - q^6 + q^5 - (\bar{s}+1)q^3}{(\bar{s}+1)q^3(q^3+1)}$.

Then by Theorem 2.2 we have

$$\text{Aut}(\bar{C}) \cong (\text{Aut}_{\mathbb{F}_{q^6}, \bar{D}, \bar{G}}^+(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

By Remark 2.1, $\text{Aut}_{\mathbb{F}_{q^6}, \bar{D}, \bar{G}}^+(\mathcal{X}) \cong \text{Aut}_{\mathbb{F}_{q^6}, \bar{D}, \bar{G}}(\mathcal{X})$. Since $\text{Aut}(\mathcal{X})$ is defined over \mathbb{F}_{q^6} , we have that $\text{Aut}_{\mathbb{F}_{q^6}, \bar{D}, \bar{G}}^+(\mathcal{X})$ coincides with the subgroup S of $\text{Aut}(\mathcal{X})$ stabilizing the support of \bar{G} . By the discussion after Lemma 8 in [5], S is contained in the group $M \cong \text{SU}(3, q) \times C_{(q^2 - q + 1)/\delta}$ defined in [5, Lemma 8]. In particular, S contains a subgroup $\text{SU}(3, q) \times C_r$. Since s/r is coprime with $(q^2 - q + 1)/\delta$, S cannot contain any subgroup $\text{SU}(3, q) \times C_{r'}$ with $r \mid r'$ and $r' > r$. The claim follows. \square

4.2 Second construction

Let $\tilde{m}, \tilde{s} \in \mathbb{N}$ and take $\tilde{s} + 1$ distinct elements $c_0 = 0, c_1, \dots, c_{\tilde{s}} \in \Gamma_0$. Define the sets

$$\tilde{\mathcal{G}} := \left(\bigcup_{i=0}^{\tilde{s}} (\mathcal{X} \cap \zeta_{c_i}) \right) \setminus \{P_\infty\}, \quad \tilde{\mathcal{D}} := \mathcal{X}(\mathbb{F}_{q^6}) \setminus \tilde{\mathcal{G}}$$

and the \mathbb{F}_{q^6} -divisors

$$\tilde{G} := \sum_{P \in \tilde{\mathcal{G}}, P \neq P_\infty} \tilde{m}P, \quad \tilde{D} := \sum_{P \in \tilde{\mathcal{D}}} P,$$

which have degree $\tilde{m}(\tilde{s} + 1)q^3$ and $q^8 - q^6 + q^5 - (\tilde{s} + 1)q^3 + 1$, respectively. Denote by $\tilde{C} := C_{\mathcal{L}}(\tilde{D}, \tilde{G})$ the associated functional AG code over \mathbb{F}_{q^6} having length $\tilde{n} = \deg \tilde{D}$, dimension \tilde{k} , and minimum distance \tilde{d} . The designed minimum distance of \tilde{C} is

$$\tilde{d}^* = \tilde{n} - \deg \tilde{G} = q^8 - q^6 + q^5 - (\tilde{m} + 1)(\tilde{s} + 1)q^3 + 1$$

Proposition 4.5. *Whenever $\tilde{d}^* > 0$, \tilde{C} attains the designed minimum distance \tilde{d}^* .*

Proof. Since $\tilde{d}^* > 0$, there exist $\tilde{m}(\tilde{s} + 1)$ distinct elements $\gamma_1, \dots, \gamma_{\tilde{m}(\tilde{s} + 1)} \in \Gamma_0 \setminus \{c_0, c_1, \dots, c_{\tilde{s}}\}$. Consider the function

$$\tilde{f} := \prod_{i=0}^{\tilde{s}} \prod_{j=1}^{\tilde{m}} \left(\frac{z - \gamma_{i\tilde{m}+j}}{z - c_i} \right).$$

The pole divisor of \tilde{f} is $(f)_{\infty} = \tilde{G}$, thus $\tilde{f} \in \tilde{G}$. The weight of $e_{\tilde{D}}(\tilde{f})$ is

$$w(e_{\tilde{D}}(\tilde{f})) = \tilde{n} - \tilde{m}(\tilde{s} + 1)q^3 = \tilde{d}^*.$$

□

Proposition 4.6. *If $\frac{q^5 - 2q^3 + q^2 - 1}{(\tilde{s} + 1)q^3} \leq \tilde{m} \leq \frac{q^5 - q^3 + q^2}{\tilde{s} + 1} - 1$, then*

$$\tilde{k} = \tilde{m}(\tilde{s} + 1)q^3 - \frac{1}{2}(q^5 - 2q^3 + q^2 - 4).$$

Proof. The proof is analogous to the proof of Proposition 3.3. □

Lemma 4.7. *Let $\tilde{m} \geq 2$ and $p \nmid \tilde{m}$. For any $P, Q \in \mathcal{X}$, $\ell(\tilde{G} - P) = \ell(\tilde{G}) - 1$ and $\ell(\tilde{G} - P - Q) = \ell(\tilde{G}) - 2$.*

Proof. As in the proof of Lemma 3.5, it suffices to provide two \mathbb{F}_{q^6} -linearly independent functions $f_1, f_2 \in \mathcal{L}(\tilde{G})$ such that $f_1, f_2 \notin \mathcal{L}(\tilde{G} - P - Q)$ and $f_1 + \lambda f_2 \notin \mathcal{L}(\tilde{G} - P - Q)$ for any $\lambda \in \mathbb{F}_{q^6}$.

- Case $P, Q \neq P_{\infty}$. Argue as in the proof of Lemma 4.3.
- Case $P = P_{\infty}, P \neq Q$. Choose $f_1 = \frac{z - \alpha}{z}$ and $f_2 = \frac{z - \beta}{z}$, with $\alpha, \beta \neq 0, \alpha \neq \beta$.
- Case $P = Q = P_{\infty}$. Choose $f_1 = \left(\frac{z - \alpha}{z}\right)^m$ and $f_2 = \left(\frac{z - \beta}{z}\right)^m$, with $\alpha, \beta \neq 0, \alpha \neq \beta$; since $p \nmid \tilde{m}$, we have $f_1 + \lambda f_2 \notin \mathcal{L}(\tilde{G} - 2P_{\infty})$.

□

Proposition 4.8. *Let $2 \leq \tilde{m} \leq \frac{q^2-1}{\tilde{s}+1} - \frac{\tilde{s}}{(\tilde{s}+1)(q^3+1)}$ with $p \nmid \tilde{m}$, and $r := \gcd\left(s, \frac{q^2-q+1}{\delta}\right)$ where $\delta := \gcd(3, q+1)$. Suppose that $\{c_1, \dots, c_{\tilde{s}}\}$ is closed under the Frobenius map $c_i \mapsto c_i^p$ and under the scalar map $\Lambda : c_i \mapsto \lambda c_i$, where $\lambda^r = 1$. Then the automorphism group of \tilde{C} is*

$$\text{Aut}(\tilde{C}) \cong (\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

If $\tilde{s} = 0$, then $\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}(\mathcal{X})$ has a normal subgroup N of index δ with

$$N \cong (Q_{q^3} \rtimes H_{q^2-1}) \times C_{(q^2-q+1)/\delta};$$

if $\tilde{s} > 0$, then

$$\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}(\mathcal{X}) \cong (Q_{q^3} \rtimes H_{q^2-1}) \times C_r.$$

Here, Q_{q^3} has order q^3 and is the unique Sylow p -subgroup of $\text{Aut}(\tilde{C})$. The groups H_i and C_j are cyclic of order i and j , respectively.

Proof. As in the proof of Proposition 3.6, the following facts hold.

- The divisor \tilde{G} is effective.
- By Lemma 4.7, $\ell(\tilde{G} - P) = \ell(\tilde{G}) - 1$ and $\ell(\tilde{G} - P - Q) = \ell(\tilde{G}) - 2$ for any $P, Q \in \mathcal{X}$.
- The functions $x' := x/z^2, z' := 1/z \in \mathcal{L}(\tilde{G})$ generate the function field of the plane model $\Pi(\mathcal{X})$ of \mathcal{X} given in [5, Theorem 4].
- The curve \mathcal{X} is defined over \mathbb{F}_p .
- The Frobenius morphism $\Phi_p : (x, z) \mapsto (x^p, y^p)$ on $\Pi(\mathcal{X})$ preserves the support of \tilde{D} .
- Since $\tilde{m} \leq \frac{q^2-1}{\tilde{s}+1} - \frac{\tilde{s}}{(\tilde{s}+1)(q^3+1)}$, we have $\tilde{n} > \deg(\tilde{G}) \cdot \deg(\Pi(\mathcal{X}))$.

Then by Theorem 2.2 we have

$$\text{Aut}(\tilde{C}) \cong (\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}^+(\mathcal{X}) \rtimes \text{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

By Remark 2.1, $\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}^+(\mathcal{X}) \cong \text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}(\mathcal{X})$. Since $\text{Aut}(\mathcal{X})$ is defined over \mathbb{F}_{q^6} , we have that $\text{Aut}_{\mathbb{F}_{q^6}, \tilde{D}, \tilde{G}}^+(\mathcal{X})$ coincides with the subgroup S of $\text{Aut}(\mathcal{X})$ stabilizing the support of \tilde{G} .

The claim follows by the properties of $\text{Aut}(\mathcal{X})$ proved in [5]. In particular, suppose $\tilde{s} = 0$. Then $\text{supp}(\tilde{G}) \cup \{P_\infty\}$ is a unique orbit of $\text{Aut}(\mathcal{X})$ by [5, Theorem 7]; hence, S is the stabilizer of P_∞ in $\text{Aut}(\mathcal{X})$, and the claim follows. Now suppose $\tilde{s} > 0$. Then S is contained in the subgroup $(Q_{q^3} \rtimes H_{q^2-1}) \times C_{(q^2-q+1)/\delta}$ of the group $M \cong \text{SU}(3, q) \times C_{(q^2-q+1)/\delta}$ defined in [5, Lemma 8]. By the hypothesis on Λ , S contains a subgroup $(Q_{q^3} \rtimes H_{q^2-1}) \times C_r$. Since h is coprime with $(q^2 - q + 1)/\delta$, S does not contain any cyclic group $C_{r'}$ with $C_r \subseteq C_{r'}$ and $r' > r$. The claim follows. \square

References

- [1] A.S. Castellanos and G.C. Tizzioti *Two-Point AG Codes on the GK Maximal Curves*, IEEE Trans. Inf. Theory **62**(2), 681–686 (2016).
- [2] A. Eid, H. Hasson, A. Ksir, and J. Peachey, *Suzuki-invariant codes from the Suzuki curve*, Des. Codes Cryptogr. **81**, 413–425 (2016).
- [3] S. Fanali and M. Giulietti, *One-Point AG Codes on the GK Maximal Curves*, IEEE Trans. Inf. Theory **56**(1), 202–210 (2010).
- [4] M. Giulietti and G. Korchmáros, *On automorphism groups of certain Goppa codes*, Des. Codes Cryptogr. **48**, 177–190 (2008).
- [5] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343**, 229–245 (2009).
- [6] V.D. Goppa, *Codes on algebraic curves*, Dokl. Akad. NAUK, SSSR **259**, 1289–1290 (1981).
- [7] V.D. Goppa, *Algebraic-geometric codes*, Izv. Akad. NAUK, SSSR **46**, 75–91 (1982).
- [8] J.P. Hansen, *Codes on the Klein quartic, ideals and decoding*, IEEE Trans. Inf. Theory **33**(6), 923–925 (1987).
- [9] C. Heegard, J. Little, and K. Saints, *Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes*, IEEE Trans. Inf. Theory **41**, 1752–1761 (1995).
- [10] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd edn. Oxford University Press, Oxford (1998).
- [11] D. Joyner, *An error-correcting codes package*, SIGSAM Comm. Computer Algebra **39**(2), 65–68 (2005).
- [12] D. Joyner and A. Ksir, *Automorphism groups of some AG codes*, IEEE Trans. Inf. Theory **52**(7), 3325–3329 (2006).
- [13] G. Korchmáros and P. Speziali, *Hermitian Codes with automorphism group isomorphic to $PGL(2, q)$ with q odd*, submitted.
- [14] G.L. Matthews, *Codes from the Suzuki function field*, IEEE Trans. Inf. Theory **50**(12), 3298–3302 (2004).

- [15] G.L. Matthews, *Weierstrass semigroups and codes from a quotient of the Hermitian curve*, Des. Codes Cryptogr. **37**, 473–492 (2005).
- [16] O. Pretzel, *Codes and Algebraic Curves*, Oxford Lecture Series in Mathematics and its Applications, **8**. The Clarendon Press, Oxford University Press, xii+192 pp. New York, (1998).
- [17] H. Stichtenoth, *A note on Hermitian codes over $GF(q^2)$* , IEEE Trans. Inf. Theory **34**(5), 1345–1348 (1988).
- [18] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics **254**, Springer, Berlin (2009).
- [19] H.J. Tiersma, *Remarks on codes from Hermitian curves*, IEEE Trans. Inf. Theory **33**(4), 605–609 (1987).
- [20] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Amsterdam (1991).
- [21] C.P. Xing and S. Ling, *A class of linear codes with good parameters from algebraic curves*, IEEE Trans. Inf. Theory **46**(4), 1527–1532 (2000).
- [22] C.P. Xing and H. Chen, *Improvements on parameters of one-point AG codes from Hermitian curves*, IEEE Trans. Inf. Theory **48**(2), 535–537 (2002).
- [23] K. Yang and P.V. Kumar, *On the true minimum distance of Hermitian codes*, Coding Theory and Algebraic Geometry **1518**, Lecture Notes in Math., 99–107 (1992).